UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,310	06/26/2001	Zheng Qi	BRCMP013B	2328

23363 7590 09/30/2004

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,310	QI ET AL.	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/30/2002, 10/6/20*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-67 are presented for examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 5-12, 15, 17-24, 26-33, 35-40, 43-46, 48-49, 51-52, 55-58, 60-61, and 63-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (Kanda, U.S. Patent No. 6,769,063 B1) in view of Callum (U.S. Patent No. 6,320,964 B1).

3.1 As per claim1, Kanda teaches a cryptography engine for performing cryptographic operations on a data block (Kanda Col. 1 lines 8-15), the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations (Kanda Col. 7 lines 11-25);

the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block (Kanda Col. 15 lines 8-20, Fig. 8A-8D);

the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block (Kanda Col. 1 lines 31-46).

Kanda does not explicitly teach multiplexer circuitry having an input stage and an output stage;

expansion logic coupled to the input stage of the multiplexer circuitry;

the output of the expansion logic is coupled to the input stage of the multiplexer circuitry;

permutation logic coupled to the expansion logic;

However Callum teaches multiplexer circuitry having an input stage and an output stage (Callum Fig. 3 No. 32, 48, & 64)

expansion logic coupled to the input stage of the multiplexer circuitry (Callum Fig. 3 No. 319, & 330);

the output of the expansion logic is coupled to the input stage of the multiplexer circuitry (Callum Fig. 3 No. 319, & 330);

permutation logic coupled to the expansion logic (Callum Fig. 3 No. 319, & 320);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Callum with in the system of Kanda because it would allow to handle instruction-intensive bit permutations to a cryptographic accelerator (Callum Abstract), by producing a 48-bit outgoing data block based on a 32-bit incoming data block, expanding from 32-bit width to a 48-bit outgoing data block, and accomplishing permutation by selection function (Callum Col. 5 lines 59-67).

3.2 As per claim 22, Kanda teaches a cryptography engine for performing cryptographic operations on a data block (Kanda Col. 1 lines 8-15), the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations (Kanda Col. 7 lines 11-25);

the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block (Kanda Col. 15 lines 8-20, Fig. 8A-8D);

the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block (Kanda Col. 1 lines 31-46);

the inverse permutation logic performs the reverse operations of the permutation logic (Kanda Col. 1 lines 62-67).

Kanda does not explicitly teach multiplexer circuitry having an input stage and an output stage;

expansion logic coupled to the multiplexer circuitry;

permutation logic coupled to the expansion logic;

However Callum teaches multiplexer circuitry having an input stage and an output stage (Callum Fig. 3 No. 32, 48, & 64);

expansion logic coupled to the multiplexer circuitry (Callum Fig. 3 No. 319, & 330);

permutation logic coupled to the expansion logic (Callum Fig. 3 No. 319, & 320);

inverse permutation logic coupled to the input stage of the multiplexer circuitry (Callum Fig. 3 No. 311, 64, & 330);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Callum with in the system of Kanda because it would allow to handle instruction-intensive bit permutations to a cryptographic accelerator (Callum Abstract), by producing a 48-bit outgoing data block based on a 32-bit incoming data block, expanding from 32-bit width to a 48-bit outgoing data block, and accomplishing permutation by selection function (Callum Col. 5 lines 59-67). And the Inverse permutation output coupled to the multiplexer circuitry would allow to produce an outgoing data block having a different bit order than the incoming data block (Callum Col. 4 lines 8-28).

3.3 As per claim 44, Kanda teaches an integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, the integrated

circuit layout providing information for configuring the cryptography engine (Kanda Col. 1 lines 8-15), the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations (Kanda Col. 7 lines 11-25);

the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block (Kanda Col. 15 lines 8-20, Fig. 8A-8D);

the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block (Kanda Col. 1 lines 31-46).

Kanda does not explicitly teach multiplexer circuitry having an input stage and an output stage;

expansion logic coupled to the input stage of the multiplexer circuitry;

the output of the expansion logic is coupled to the input stage of the multiplexer circuitry;

permutation logic coupled to the expansion logic;

However Callum teaches multiplexer circuitry having an input stage and an output stage (Callum Fig. 3 No. 32, 48, & 64);

expansion logic coupled to the input stage of the multiplexer circuitry (Callum Fig. 3 No. 319, & 330);

the output of the expansion logic is coupled to the input stage of the multiplexer circuitry (Callum Fig. 3 No. 319, & 330);

permutation logic coupled to the expansion logic (Callum Fig. 3 No. 319, & 320);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Callum with in the system of Kanda because it would allow to handle instruction-intensive bit permutations to a cryptographic accelerator (Callum Abstract), by producing a 48-bit outgoing data block based on a 32-bit incoming data block, expanding from 32-bit width to a 48-bit outgoing data block, and accomplishing permutation by selection function (Callum Col. 5 lines 59-67).

3.4 As per claim 56, Kanda teaches an integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine (Kanda Col. 1 lines 8-15), the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations (Kanda Col. 7 lines 11-25);

the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block (Kanda Col. 15 lines 8-20, Fig. 8A-8D);

the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block (Kanda Col. 1 lines 31-46);

the inverse permutation logic performs the reverse operations of the permutation logic (Kanda Col. 1 lines 62-67).

Kanda does not explicitly teach multiplexer circuitry having an input stage and an output stage;

expansion logic coupled to the multiplexer circuitry;

permutation logic coupled to the expansion logic;

inverse permutation logic coupled to the input stage of the multiplexer circuitry,

However Callum teaches multiplexer circuitry having an input stage and an output stage (Callum Fig. 3 No. 32, 48, & 64);

expansion logic coupled to the multiplexer circuitry (Callum Fig. 3 No. 319, & 330);

permutation logic coupled to the expansion logic (Callum Fig. 3 No. 319, & 320);

inverse permutation logic coupled to the input stage of the multiplexer circuitry (Fig. 3 No. 311, 64, & 330);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Callum with in the system of Kanda because

it would allow to handle instruction-intensive bit permutations to a cryptographic accelerator (Callum Abstract), by producing a 48-bit outgoing data block based on a 32-bit incoming data block, expanding from 32-bit width to a 48-bit outgoing data block, and accomplishing permutation by selection function (Callum Col. 5 lines 59-67). And the Inverse permutation output coupled to the multiplexer circuitry would allow to produce an outgoing data block having a different bit order than the incoming data block (Callum Col. 4 lines 8-28).

3.5 As per claims 2, 23, 45, and 57, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic (Kanda Col. 10 lines 51- col. 11 lines 15, Col. 3 lines 31-52).

3.6 As per claims 3, 24, 46, and 58, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the cryptography engine is a DES engine (Kanda Col. 14 lines 15-28).

3.7 As per claims 5, and 26, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the first bit sequence is less than 32 bits (Kanda Col. 2 lines 1-21).

3.8 As per claims 6, 27, 48, and 60, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the first bit sequence is four bits (Kanda Col. 17 lines 9-28).

3.9 As per claims 7, and 28, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the expanded first bit sequence is less than 48 bits (Kanda Fig. 10).

3.10 As per claims 8, 29, 49, and 61, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the expanded first bit sequence is less than six bits (Kanda Col. 17 lines 9-28).

3.11 As per claims 9, and 30, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the third bit sequence is less than 48 bits (Kanda Col. 2 lines 22-39).

3.12 As per claims 10, and 31, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the third bit sequence is six bits (Kanda Col. 2 lines 22-39).

3.13 As per claims 11, and 32, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the second bit sequence is less than 32 bits (Kanda Col. 2 lines 1-21, col. 10 lines 22-35).

3.14 As per claims 12, and 33, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the second bit sequence is four bits (Kanda Col. 10 lines 22-35, col. 15 lines 20-53).

3.15 As per claims 15, 43, 55, and 67, Kanda and Callum teach all the subject matter as described above. In addition, Callum teaches the cryptography engine, wherein the expansion logic and the permutation logic are associated with DES operations (Callum Col. 3 lines 32-47, Fig. 3 No. 319 & 320) The rational for combining are the same bases as claim 1 above.

3.16 As per claims 17, and 36, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the key scheduler comprises a determination stage (Kanda Col. 15 lines 21-33).

3.17 As per claims 18, and 37, Kanda and Callum teach all the subject matter as described above. In addition, Callum teaches the cryptography engine, wherein the key scheduler comprises a shift stage (Callum Col. 4 lines 46-col. 5 lines 5) The rational for combining is the same bases as claim 1 above.

3.18 As per claims 19, and 38, Kanda, and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the key scheduler comprises a propagation stage (Kanda Col. 2 lines 1-21).

3.19 As per claims 20, and 39, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the key scheduler comprises a consumption stage (Kanda Col. 3 lines 30-51).

3.20 As per claims 21, 40, 52, and 64, Kanda and Callum teach all the subject matter as described above. In addition, Callum teaches the cryptography engine, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value (Callum Col. 4 lines 46-55, Fig. 5)

3.21 As per claim 35, Kanda and Callum teach all the subject matter as described above. In addition, Kanda teaches the cryptography engine, wherein the key scheduler comprises a plurality of stages (Kanda Col. 1 lines 18-67).

3.22 As per claims 51, and 63, Kanda and Callum teach all the subject matter as described above. In addition Kanda teaches the cryptography engine, wherein the key scheduler comprises a determination stage (Kanda Col. 15 lines 21-53), a propagation stage (Kanda Col. 2 lines 1-21), and a consumption stage (Kanda col. 3 lines 30-51), and Callum teaches a shift stage (Callum Col. 4 lines 46-Col. 5 lines 5) The rational for combining are the same as claim 22 above.

4. Claims 4, 13-14, 25, 41-42, 47, 53-54, 59 and 65-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (Kanda, U.S. Patent No. 6,769,063 B1) in view of Callum (U.S. Patent No. 6,320,964 B1), and in further view of Steinman et al. (Steinman, U.S. Patent No. 6,591,349 B1).

4.1 As per claims 4, 25, 47, and 59, Kanda and Callum teach all the subject matter as described above.

Kanda and Callum do not explicitly teach two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level;

However Steinman teaches 2-to-1 multiplexer (Steinman Col. 4 lines 1-13);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Steinman with in the combination system of Kanda and Callum because it would allow to increase the performance of computer memory system by reducing lost clock cycles (Steinman Abstract). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level because it would allow to increase the performance of DES or triple DES engine as the performance of the computer improved in using 2-to-1 multiplexers. Speeding up the clock cycle improves the performance of DES.

4.2 As per claims 13, 41, 53, and 65, Kanda, Callum, and Steinman teach all the subject matter as described above. In addition, Steinman teaches the cryptography engine, wherein the multiplexer circuitry is a two-level multiplexer (Steinman Col. 4 lines 1-13). The rational for combining are the same as claim 4 above.

4.3 As per claims 14, 42, 54, and 66, Kanda and Callum teach all the subject matter as described above. In addition, Callum teaches the cryptography engine, wherein the multiplexer is configured to select either initial data (Callum Col. 3 lines 48-61), swapped data, or non-swapped data to provide to the output stage of the multiplexer (Callum Col. 1 lines 39-46, Fig. 3), and Steinman teaches the two-level multiplexer (Steinman Col. 4 lines 1-13). The rational for combining are the same as claim 4 above.

5. Claims 16, 34, 50, and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (Kanda, U.S. Patent No. 6,769,063 B1) in view of Callum (U.S. Patent No. 6,320,964 B1), and Steinman et al. (Steinman, U.S. Patent No. 6,591,349 B1), and in further view of Teppler (U.S. Patent No. 6,792,536 B1).

5.1 As per claims 16, 34, 50, and 62, Kanda, Callum, and Steinman teach all the subject matter as described above.

Kanda, Callum, and Steinman do not explicitly teach performing pipelined key scheduling logic.

However Teppler teaches DES pipelining (Teppler Col. 7 lines 13-25)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Teppler with in the combination system of Kanda, Callum, and Steinman because it would allow to have not impacted system performance (Teppler Col. 7 lines 13-25).

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw

Art Unit 2136

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100